EXHIBIT 1

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants and Counterclaim-Plaintiffs.	Civil Action No. 04-CV-1199 (SLR)

JOINT MOTION OF DEFENDANTS ISS AND SYMANTEC FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 & 103

Pursuant to the Court's June 30, 2005 Scheduling Order, Defendants Internet Security Systems, Inc., a Delaware corporation, Internet Security Systems, Inc., a Georgia corporation (collectively "ISS") and Symantec Corporation, a Delaware corporation ("Symantec"), move pursuant to Fed. R. Civ. P. 56, for an Order granting summary judgment that the asserted claims of the four patents-in-suit assigned to Plaintiff SRI International ("SRI") are invalid under 35 U.S.C. §§ 102 and 103.

Dated: June 16, 2006

POTTER ANDERSON & CORROON LLP

/s/ Richard L. Horwitz
Richard L. Horwitz (#2246)
David E. Moore (#3983)
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19899
Tel.: (302) 984-6000
Fax: (302) 658-1192
rhorwitz@potteranderson.com
dmoore@potteranderson.com

OF COUNSEL:

Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
1180 Peachtree Street
Atlanta, GA 30309
Tel: (404) 572-4600
Fax: (404) 572-51345

Theresa A. Moehlman
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100
Fax: (212) 556-2222

Attorneys for Defendant
INTERNET SECURITY SYSTEMS, INC.,
a Delaware Corporation and
INTERNET SECURITY SYSTEMS, INC.,
a Georgia Corporation

MORRIS, JAMES, HITCHENS & WILLIAMS, LLP

/s/ Mary B. Matterer
Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
Tel.: (302) 888-6800
rherrmann@morrisjames.com
mmatterer@morrisjames.com

OF COUNSEL:

Lloyd R. Day, Jr.
Robert M. Galvin
Paul S. Grewal
DAY, CASEBEER MADRID & BATCHELDER LLP
20300 Stevens Creek Blvd.,
Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

Attorneys for Defendant
SYMANTEC CORPORATION

CERTIFICATE OF SERVICE

I hereby certify that on the 16th day of June, 2006, I electronically filed the foregoing document, **JOINT MOTION OF DEFENDANTS ISS AND SYMANTEC FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 & 103**, with the Clerk of the Court using CM/ECF which will send notification of such filing to the following:

John F. Horvath, Esq.
Fish & Richardson, P.C.
919 North Market Street, Suite 1100
Wilmington, DE 19801

Richard L. Horwitz, Esq.
David E. Moore, Esq.
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
Wilmington, DE 19801

Additionally, I hereby certify that on the 16th day of June, 2006, the foregoing document was served via email and via federal express on the following non-registered participants:

Howard G. Pollack, Esq.
Michael J. Curley, Esq.
Fish & Richardson
500 Arguello Street, Suite 500
Redwood City, CA 94063
650.839.5070

Holmes Hawkins, III, Esq.
King & Spalding
1180 Peachtree Street
Atlanta, GA 30309-3521
404.572.4600

Theresa Moehlman, Esq.
King & Spalding LLP
1185 Avenue of the Americas
New York, NY 10036-4003
212.556.2100

/s/Mary B. Matterer
Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
Morris, James, Hitchens & Williams LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
(302) 888-6800
rherrmann@morrisjames.com
mmatterer@morrisjames.com
Counsel for Defendant Symantec Corporation

EXHIBIT 2

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants and Counterclaim-Plaintiffs.	Civil Action No. 04-CV-1199 (SLR)

OPENING BRIEF IN SUPPORT OF JOINT MOTION FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 & 103 OF DEFENDANTS ISS AND SYMANTEC

Richard L. Horwitz (#2246)
David E. Moore (#3983)
POTTER ANDERSON & CORROON LLP
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19899
Tel.: (302) 984-6000
Fax: (302) 658-1192

OF COUNSEL:
Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
1180 Peachtree Street
Atlanta, GA 30309
Tel: (404) 572-4600
Fax: (404) 572-5134

Theresa A. Moehlman
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100
Fax: (212) 556-2222

Attorneys for Defendant
INTERNET SECURITY SYSTEMS, INC., a Delaware Corporation and INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation

Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
MORRIS, JAMES, HITCHENS & WILLIAMS, LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
Tel.: (302) 888-6800

OF COUNSEL:
Lloyd R. Day, Jr.
Robert M. Galvin
Paul S. Grewal
DAY, CASEBEER MADRID & BATCHELDER LLP
20300 Stevens Creek Blvd.,
Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

Attorneys for Defendant
SYMANTEC CORPORATION

Table of Contents

I. STATEMENT OF THE CASE

In this action, SRI International, Inc. ("SRI") has sued Defendants Internet Security Systems, Inc., a Delaware corporation, Internet Security Systems, Inc., a Georgia corporation (collectively "ISS") and Symantec Corporation, a Delaware corporation ("Symantec") for patent infringement.[1] At issue are four patents relating to network intrusion detection.[2] All of the patents-in-suit claim the same priority date of November 9, 1998 and all share an almost identical written disclosure. Phillip Porras and Alfonso Valdes, employees of SRI, are the named inventors on all four patents.

The patents-in-suit generally relate to detecting attacks on computer networks, a field known as intrusion detection. There are two main facets to the patents-in-suit: (1) a hierarchy of monitors for detecting suspicious network activity, and (2) a statistical algorithm for use in detecting attacks. The '338 claims focus upon the statistical algorithm, the '203 and '615 claims focus upon the hierarchical monitor architecture, and the '212 claims include both facets.

These patents result from SRI's work on a system called EMERALD, which was funded by the United States government under the auspices of the Defense Advanced Research Projects Agency ("DARPA"). DARPA funded several projects on intrusion detection during the early-to-mid 1990s. In addition to EMERALD, DARPA also funded

---

[1] All referenced exhibits are attached to the Declaration of Renee DuBord Brown.

[2] The patents-in-suit are U.S. Patent Nos. 6,321,338 ("the '338 patent") [Ex. A]; [redacted] 6,484,203 ("the '203 patent") [Ex. C]; and 6,711,615 ("the '615 patent") [Ex. D]. SRI has asserted different sets of claims against each Defendant. For convenience, the superset of asserted claims is addressed herein, which encompasses: '338 claims 1-2, 4-5, 11-13, 18-19, 24; [redacted]

a system called JiNao, which was developed at North Carolina State University and an associated company called MCNC. The named inventors of the patents-in-suit collaborated on JiNao. Both EMERALD and JiNao adopted a statistical algorithm that had been developed at SRI in the late 1980s/early 1990s. Both EMERALD and JiNao applied this algorithm to network traffic data. Both EMERALD and JiNao employed hierarchical network monitors.

During the course of their work on EMERALD and JiNao, the researchers shared the fruits of their government-funded research with the public by publishing detailed papers describing these systems. These public disclosures pre-date the priority filing date of the patents-in-suit by more than one year and describe all elements of the patent claims at issue. As a result, these printed publications invalidate the claims-in-suit.

SRI is not entitled to patent claims that would exclude others from practicing what had already been placed in the public domain. Under 35 U.S.C. § 102 (b), a patent is invalid if it claims inventions that were described in a printed publication more than one year before the filing date of the patent application. This rule applies equally to any public disclosure – including prior disclosures by the very person who later seeks a patent. The patent laws are designed to promote technological advances, not takings from the public domain. *See Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141, 148-49 (1989). If an inventor shares his invention with the public and does not file for patent protection within one year, the invention is dedicated to the public. Here, the named inventors filed their patent application in November 1998, but described the claimed subject matter in at least two publications dated more than one year before that filing date. In addition, the developers of the JiNao system also published their paper describing the claimed subject matter more than one year before that filing date. The

inventors are therefore not entitled to patents on these claims.

[redacted]

[redacted]

Finally, the publication describing the JiNao system was published in April 1997. *See* Y. Frank Jou et al., *Architecture Design of a Scalable Intrusion Detection System for the Emerging Network Infrastructure*, Technical Report, April 1997 ("*JiNao Report*") [Ex. J]. The *JiNao Report* disclosed the hierarchical architecture claims of the '203, '615 and '212 patents. The *JiNao Report* also described the same statistical detection algorithm used by SRI's EMERALD system and claimed in the '338 patent. In fact, the SRI EMERALD team collaborated with the JiNao team regarding the implementation of the algorithm, as well as their related DARPA programs. Despite their collaboration with the JiNao researchers and their awareness of the *JiNao Report*, SRI's named inventors failed to disclose the *JiNao Report* to the United States Patent and Trademark Office ("US PTO").

Resolution of this case in its entirety on summary judgment is appropriate. The text of the printed publications upon which Defendants rely cannot be disputed. The dates of publication of these prior art references are beyond genuine dispute. The similarity, if not identity, of the description between these prior art publications and the patents-in-suit can also not be genuinely disputed, and have been largely conceded by the inventors and SRI's expert. [redacted]

[redacted]

[redacted] In the case of the *JiNao Report*, the authors actually collaborated with the inventors and used the very same statistical algorithms at the heart of the system described in the patents-in-suit. Based on these undisputed facts, summary judgment of invalidity on all asserted claims should be entered.

Furthermore, this summary judgment motion does not in any way rest upon the outcome of the claim construction in this case. This unique situation is due to the fact that *Emerald 1997* and *Live Traffic* were written by the inventors about the same system discussed in the patents-in-suit, and thus the language used is virtually identical. Similarly, the *JiNao Report* also uses similar language to describe the JiNao statistical algorithms because the JiNao team used the same algorithms as SRI disclosed in the patents-in-suit. Thus, the references relied upon herein are invalidating references regardless of whether SRI's or the Defendant's proposed constructions are adopted.

II. SUMMARY OF THE ARGUMENT

[redacted]

5. The *JiNao Report* anticipates pursuant to 35 U.S.C. § 102 (b) the '338, [redacted] asserted claims.

III. STATEMENT OF FACTS

A. BACKGROUND REGARDING INTRUSION DETECTION

1. The history of the intrusion detection field

Intrusion detection systems ("IDS") are designed to detect, and in some cases thwart, unwanted attempts to infiltrate or access a computer or computer network. An "intrusion" can refer to any type of anomalous, illicit, or prohibited activity. An intrusion may originate from an external threat, or misuse by an internal user. IDS has been described as "a burglar alarm for computers and networks." R. Bace, INTRUSION DETECTION at 7 (Macmillan Technical Publishing 2000) [Ex. Z]. Like any technology, the IDS field has evolved over time. In order to provide a context for understanding the claimed inventions, this section provides a short overview of the history of the IDS field.

The U.S. government has played an important role. Beginning in the 1970's, the Department of Defense ("DOD") funded a "trusted systems" initiative to provide computer system security for the processing of classified information. As part of this program, the DOD created a policy for implementing certain auditing functions for computers to track behavior and discover potential security problems. *See* R. Bace, INTRUSION DETECTION at 11 [Ex. Z]. An audit trail (also known as an "audit log") is a record showing who has accessed a computer system and what operations he or she has performed during a given period of time. An audit trail may track basic operating system functions, such as system calls and processes performed, or it may track application usage or data access.[5]

[5] For an overview regarding audit trails, *see* S. Garfinkel and G. Spafford, PRACTICAL

Many early IDS systems focused upon the analysis of audit trail information. Such analysis is sometimes referred to as "host-based" because it relies upon information generated on a particular "host" or computer. However, with the proliferation of large computer networks and the likelihood of network-based attacks increasing, IDS systems began focusing upon network traffic and network sources for attack. For example, in the early 1990's, the Network Security Monitor ("NSM") developed at the University of California at Davis targeted computer networks and analyzed packet data. *See id.* at 18-19 [Ex. Z]; L.T. Heberlein et al., *A Network Security Monitor*, Proceedings of the 1990 IEEE Computer Society Symposium on Research in Security and Privacy, at 296-304, Oakland, C.A., May 7-9, 1990 [Ex. NN].

As the inventors of the patents-in-suit have acknowledged, analysis of packet data in the context of network monitoring is quite old, and has been studied extensively in both the IDS field and many other areas of computing.[6] Packet-switched networks were first developed by the DOD for the Advanced Research Projects Agency Network ("ARPANET") in the late 1960s, which eventually formed the backbone of the Internet we know today. In the 1970-80s, early Internet researchers began developing a standard communication protocol for the Internet. This protocol suite became known as TCP/IP ("Transmission Control Protocol/Internet Protocol").[7]

UNIX & INTERNET SECURITY at 289-92 (O'Reilly and Assoc. 2nd ed. 1996) [Ex. AA].

[6] The inventors have stated in their publications that the concepts of network monitoring and the use of packet monitoring in IDS were not new at the time of the alleged inventions. *See* P. Porras and A. Valdes, *Live Traffic* at 3 (noting that "[n]etwork monitoring, in the context of fault detection and diagnosis for computer network and telecommunication environments, has been studied extensively by the network management and alarm correlation community" and "[b]oth [the NSM and NADIR systems] performed broadcast LAN packet monitoring to analyze traffic patterns for known hostile or anomalous activity") [Ex. I].

[7] *See* B. M. Leiner et al., A Brief History of the Internet,

In conjunction with the growth of the Internet, a wide variety of different types of computer and networking hardware were developed to handle the routing, monitoring, and filtering of network traffic and network packets. For example, routers and gateways were developed to connect computer networks. Routers and gateways receive packets and forward them to their correct destinations based upon the address in each packet's header.[8] As the need for securing networks, especially those connected across the Internet, became apparent, "firewalls" were developed in the early 1990's to provide a mechanism to filter and block unwanted packets and traffic.[9] Firewalls and the information they generate serve as important data sources for IDS systems.[10]

2. History of SRI's IDES, NIDES and EMERALD projects

[redacted]

http://www.isoc.org/internet/history/brief.shtml (last visited June 15, 2006).

[8] Although these two terms have been used synonymously, a gateway has also been defined as connecting networks using different communication protocols. *See* definitions of "router" and "gateway" in COMPUTER DICTIONARY, Microsoft Press 3rd ed. (1997) [Ex. LL].

[9] *See* Avolio Decl., ¶ 24 [Ex. X].

[10] "Many firewalls, I&A systems, access control systems, and other security devices and subsystems generate their own activity logs. These logs contain information that is, by definition, of security significance; they are therefore of particular value to the intrusion detection process. Including these logs as information sources is an obvious way to improve the quality of the intrusion detection process." R. Bace, INTRUSION DETECTION at 74 [Ex. Z].

Pages 9 and 10

Redacted

[redacted]

3. History of JiNao

The *JiNao Report* also stems from work related to SRI's NIDES project. The EMERALD and JiNao projects were both government projects funded by DARPA reporting to the same Program Manager.[18] The JiNao team used SRI's NIDES statistical algorithms for analysis – the same algorithms the patents-in-suit refer to as being suitable for use in the patented system. *See JiNao Report* at 18 [Ex. J] and '338 col. 5:42-48 [Ex. A]. Multiple meetings between the named inventors and the JiNao team occurred at which the use of the NIDES algorithms was discussed.[19] Reports on EMERALD for the U.S. Government written by the inventors confirm that the inventors provided information on the EMERALD statistical component to the JiNao team.[20]

Like EMERALD, the disclosed JiNao system included an analysis hierarchy of monitors, where each monitor used a statistical-based and a rule-based analysis engine.

[redacted]

[18] Porras 30(b)(6) Tr. 96-100 [Ex. T]; Jou Tr. 96-97 [Ex. R]; Lunt Tr. 16-17; 80-81 [Ex. KK].

[19] Jou Tr. 30-31, 39-42, 66-67, 69-70 [Ex. R]; Porras Tr. 163, 174-75 [Ex. T]; Valdes Tr. 86-88, 156-57 [Ex. U].

[20] *See* SRI 011739-43 at SRI 011742 and SRI 012308-404 at SRI 012400 [Ex. EE]; *see*

Like EMERALD, JiNao applied the NIDES statistical detection algorithm to network traffic data.

B. The Alleged Inventions of the Patents-in-Suit

The common specification of the patents-in-suit describes a hierarchical scheme for the monitoring and analysis of networks for the purpose of intrusion detection.[21] The specification describes two different types of "analysis engines" for the network monitors: a "profiler engine" which uses a particular statistical technique, and a "signature engine." The '338 claims focus upon statistical profiling, which the specification explains uses SRI's prior techniques from the NIDES program:

> The profile engine 22 may use a statistical analysis technique described in A. Valdes and D. Anderson, "Statistical Methods for Computer Usage Anomaly Detection Using NIDES", Proceedings of the Third International Workshop on Rough Sets and Soft Computing, January 1995, which is incorporated by reference in its entirety.

'338 col. 5:42-48 [Ex. A].[22] [redacted]

also Jou Tr. 30-31, 47, 67 [Ex. R].

[redacted]

[22] This publication is referred to herein as *Statistical Methods, see* Ex. FF.

The specification describes an enterprise network which includes a set of "network monitors" for analyzing network activity. '338 col. 3:32-35 [Ex. A]. These monitors are deployed in a hierarchy and include lowest-level "service monitors," as well as "domain monitors" and "enterprise monitors." The service monitors analyze data from network traffic / network packets handled by "network entities" such as gateways, routers, or firewalls. '338 col. 3:42-45 [Ex. A]. The service monitors produce reports and disseminate them to other monitors via a subscription-based distribution scheme. '338 col. 3:55-65 [Ex. A].

Each monitor can analyze "event records that form an event stream." '338 col. 4:61-62 [Ex. A]. Event records can be created from raw network traffic / network packets. As the specification states, the selection of data from the packets for analysis can be based upon different criteria. '338 col. 4:61-5:5 [Ex. A]. The analysis engines of the monitors receive the event records. '338 col. 5:34-35 [Ex. A].

Each monitor includes one or more analysis engines, including a "signature analysis engine" and a "statistical analysis engine," which perform different types of analysis on the data collected by the monitors. *See* '338 Fig. 2 [Ex. A]. The signature engine looks for known patterns of attack in the event stream. For example, this engine can perform a threshold analysis, which detects when the number of occurrences of a specific event exceeds a preset level. '338 col. 7:24-26, 7:45-55 [Ex. A]. By contrast, the statistical engine performs statistical profile-based anomaly detection where the pattern of attack may not be known. The statistical engine uses "statistical measures to profile network activity indicated by an event stream." '338 col. 7:36-38 [Ex. A]. Statistical measures are variables created from event records. These measures are used to create

[23] With the exception of '615 claim 7, which requires a "statistical detection method."

both a long-term and a short-term statistical profile. '338 col. 6:38-50 [Ex. A]. While the long-term statistical profile characterizes historical activity, the short-term statistical profile "characterizes recent activity." '338 col. 6:44-47 [Ex. A]. The short-term profile is compared to the long term profile to determine if recent activity is anomalous. '338 col. 6:38-7:3 [Ex. A].

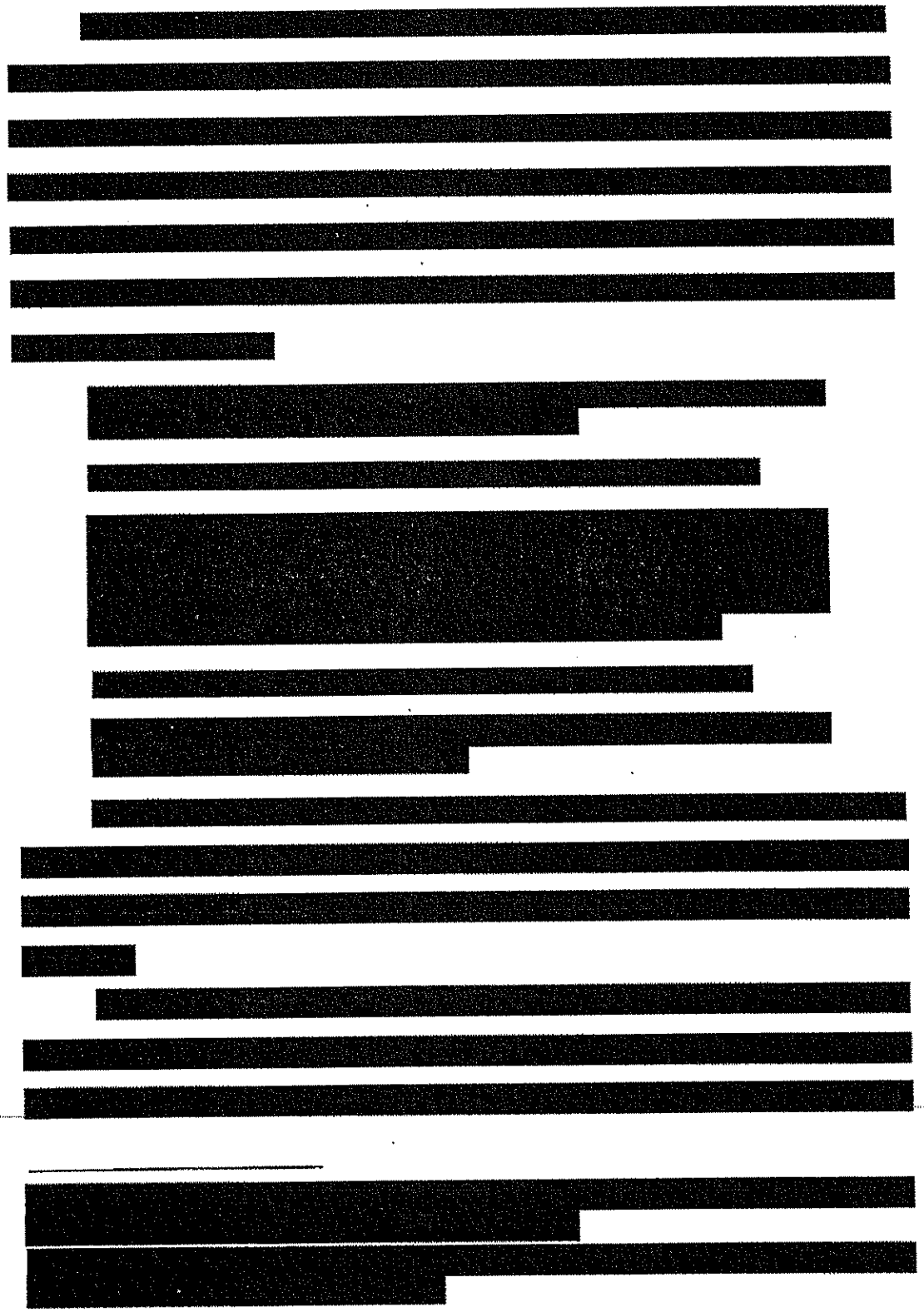
The specification mentions that hierarchical domain monitors correlate reports from service monitors and distribute their reports to enterprise monitors. '338 col. 3:66-4:18 [Ex. A]. In turn, hierarchical enterprise monitors correlate reports across their set of monitored domains. '338 col. 4:18-47 [Ex. A]. However, no description of how this "correlation" is performed is provided.

C. THE ASSERTED CLAIMS

Many of the asserted claims are duplicative. For example, although each patent has both method and apparatus claims, the limitations of each are virtually identical (*see, e.g.*, '338 claims 1 and 24).

The '338 patent claims focus on the statistical anomaly detection algorithm. Claim 1 is representative of the independent claims:

> 1. A method of network surveillance, comprising:
>
> receiving network packets handled by a network entity;
>
> building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets, the at least one measure monitoring data transfers, errors, or network connections;
>
> comparing at least one long-term and at least one short-term statistical profile; and
>
> determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.



utilize a "statistical detection method." In addition, '212 claims 2 and 3 further require the use of a "signature matching detection method."

D. THE SUMMARY OF ESTABLISHED FACTS

1. The priority filing date for all of the patents-in-suit is November 9, 1998.

[redacted]

6. *JiNao Report* was publicly available more than one year prior to November 9, 1998.[30]

[redacted]

[redacted]

[30] The author of the *JiNao Report*, Mr. Jou, testified that he made the document available on the MCNC website in April 1997. Jou Tr. 73-87 [Ex. R]. A declaration from the Internet Archive confirms that the *JiNao Report* was publicly available prior to November 1997. *See* Internet Archive Decl. at ISS_02125906, ISS_ 02125910 (illustrating that the *JiNao Report* was posted on the MCNC website at least as early as 08/01/1997) [Ex. S]. Furthermore, Mr. Jou testified he emailed a link to this document to many researchers in the intrusion detection field in April 1997, including both named inventors. Jou Tr. 75-77; Jou Exhibit 17 (SRIE 0399295) [Ex. R].

[redacted]

[redacted]

19. *JiNao Report* discloses all of the limitations of the asserted claims.[43]

[redacted]

[34] Avolio Decl. ¶¶ 21-27, 35-41, 60-78 [Ex. X].

[35] Avolio Decl. ¶¶ 35-41, 63, 67-71, 73-75, 79 [Ex. X].

[redacted]

[43] Chart comparing *JiNao Report* to the asserted claims [Ex. M]; *see also supra* Part IV.D.

20. *JiNao Report* is an enabling reference for the asserted claims.[44]

IV. SUMMARY JUDGMENT OF INVALIDITY SHOULD BE ENTERED ON ALL OF THE ASSERTED CLAIMS

A. LEGAL STANDARDS

1. Summary judgment

Summary judgment is appropriate if "no genuine issue exists as to any material fact and that the moving party is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c). "Facts that could alter the outcome are material, and disputes are genuine if evidence exists from which a rational person could conclude that the position of the person with the burden of proof on the disputed issue is correct." *Matsushita Elec. Indus. Co. v. Cinram Int'l, Inc.*, 299 F. Supp. 2d 348, 357 (D. Del. 2004) (citations omitted). The moving party bears the burden of proving that no genuine issue of material fact exists. *See Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586 n.10 (1986). If the moving party proves an absence of material fact, the nonmoving party "must come forward with 'specific facts showing that there is a genuine issue for trial.'" *Matsushita*, 475 U.S. at 587 (quoting Fed. R. Civ. P. 56(e)).

2. Anticipation under 35 U.S.C. § 102

"A patent is invalid for anticipation when the same device or method, having all the elements contained in the claim limitations, is described in a single prior art reference." *Crown Operations Int'l, Ltd. v. Solutia, Inc.*, 289 F.3d 1367, 1375 (Fed. Cir. 2002). Anticipation is a question of fact, *see In re King*, 801 F.2d 1324, 1326 (Fed. Cir. 1986), and must be proven by clear and convincing evidence. *See Norian Corp. v. Stryker Corp.*, 363 F.3d 1321, 1326 (Fed. Cir. 2004). Despite being a question of fact,

[44] Heberlein Decl. ¶¶ 94-95 [Ex. Y].

summary judgment of anticipation is appropriate if the record reveals no genuine dispute of material fact. *See General Electric Co. v. Nintendo Co., Ltd.*, 179 F.3d 1350, 1353 (Fed. Cir. 1990); *see also Telemac Cellular Corp. v. Topp Telecom, Inc.*, 247 F.3d 1316, 1327 (Fed. Cir. 2001).

In order to anticipate, a prior art disclosure must enable one of skill in the art to practice the invention without undue experimentation. *See Novo Nordisk Pharm., Inc. v. Bio-Tech. Gen. Corp.*, 424 F.3d 1347, 1355 (Fed. Cir. 2005). Whether a prior art reference is enabled is a question of law based on underlying factual findings. *Id.* at 1342-43. The patentee bears the burden to show that a prior art reference is not enabled. *See Amgen Inc. v. Hoechst Marion Roussel, Inc.*, 314 F.3d 1313, 1355 (Fed. Cir. 2003) (regarding a prior art patent); *Novo Nordisk Pharm., Inc. v. Bio-Tech. Gen. Corp.*, 2004 U.S. Dist LEXIS 14960 at *73 (D. Del. 2004) (regarding non-patent prior art) *aff'd in part and vacated in part*, 424 F.3d 1347 (Fed. Cir. 2005).

[redacted]

Pages 20 through 35

Redacted

[redacted]

D. THE JINAO REPORT ANTICIPATES THE ASSERTED CLAIMS

The *JiNao Report* was publicly available more than one year before the filing date of the patents-in-suit.[88] The *JiNao Report* described the architecture of an intrusion detection system designed for protecting against intrusions into network infrastructure such as routers. *See JiNao Report* at 1 [Ex. J]. The JiNao system performs both statistical and signature analysis of network routing and management protocol traffic.

[redacted]

[88] *See supra* note 30.

See JiNao Report at 1 [Ex. J].[89] The JiNao system's "dual analysis engine" monitor is quite similar to the dual analysis engine monitor shown in Fig. 2 of the patent specification.[90] Both monitors read in network traffic and perform statistical analysis upon that traffic looking for intrusions. In addition, both monitors use the same NIDES statistical profiling algorithms adapted for network traffic.[91]

The *JiNao Report* was not submitted to the US PTO or considered by the Examiner for any of the patents-in-suit.

1. The JiNao Report anticipates the asserted '338 claims

As shown in Exhibit M, the *JiNao Report* anticipates all of the asserted claims of the '338 patent. SRI's expert Dr. Kesidis conceded that the system described in the *JiNao Report* satisfies all of the elements of '338 claim 1:

- JiNao received network packets handled by a network entity,[92]
- JiNao built long-term statistical profiles,[93]
- JiNao built short-term statistical profiles,[94]
- JiNao used measures of network packets[95] monitoring network connections,[96]
- JiNao compared a long-term and a short-term statistical profile,[97]
- JiNao determined whether there is a significant difference between the

---

[89] Jou Tr. 24-25 [Ex. R].

[90] Compare *JiNao Report* Figure 1 at 4 with '338 Fig. 2. and '338 col. 4:48-60.

[91] *See JiNao Report* at 18 [Ex. J] and '338 col. 5:43-52 [Ex. A].

[92] Kesidis Tr. 50-51, 55-58 [Ex. V].

[93] Kesidis Tr. 52-53, 58 [Ex. V].

[94] Kesidis Tr. 53, 58 [Ex. V].

[95] Kesidis Tr. 210-212 [Ex. V].

[96] Kesidis Tr. 51, 58-59 [Ex. V]. Specifically, Dr. Kesidis conceded that the Hello packets which JiNao monitored indicate a network connection. The *JiNao Report* at 19 discloses that JiNao monitored Hello packets.

[97] Kesidis Tr. 53, 59 [Ex. V].

profiles.[98] A significant statistical deviation indicates an alert.[99]

SRI appears to be attempting to distinguish the *JiNao Report* as not satisfying the claim preamble requiring a "method of network surveillance."[100] However, a claim preamble is not a limitation of the claim if it merely recites a statement of purpose. *See Pitney Bowes, Inc. v. Hewlett-Packard Co.*, 182 F. 3d 1298, 1305 (Fed. Cir. 1999). Furthermore, SRI's expert conceded the actual claimed method was laid out in the method steps, not the preamble.[101] SRI never previously claimed this preamble constituted a claim limitation, and never requested construction of any of the terms in the preamble.[102]

However, even assuming the preamble constitutes a claim limitation, the disclosed JiNao system satisfies it. As SRI's expert admitted, the JiNao monitor receives packets from the network.[103] Furthermore, the *JiNao Report* itself makes it clear the system is designed for performing network surveillance:

> In particular, we will conduct logical and statistical **analysis of network routing and management protocols** to construct a scalable distributed intrusion detection system for the emerging internetwork environment.

JiNao Report at 1 (emphasis added) [Ex. J].

> Most of the current **network intrusion detection efforts** have taken one of the two following approaches. One approach is to collect data from separate hosts on a network for processing by a centralized intrusion

---

[98] Kesidis Tr. 54 [Ex. V].

[99] Kesidis Tr. 74 [Ex. V].

[100] Kesidis Tr. 47-50 [Ex. V].

[101] *See* Kesidis Tr. 396 [Ex. V].

[102] *See* D.I. 265 (SRI's Opening Claim Construction Brief).

[103] Kesidis Tr. 210-11 [Ex. V]; *see also JiNao Report* at 4 (Fig. 1) (showing the statistical analysis portion of the local detection module receives data from the network, and at 18, stating "[a]fter the incoming packet passes through the rule-based checking, it will be forwarded in parallel both to the protocol engine for execution and to the detection module for further analysis."). [Ex. J].

> detection system [2][3]. The other approach is **to target network traffic at the service and protocol levels** [6][7]. **Our effort is close to the second approach** with a few exceptions.

JiNao Report at 2 (emphasis added) [Ex. J].

In addition to disclosing using measures monitoring "network connections" for statistical profiling, the *JiNao Report* further disclosed using measures satisfying '338 claims 2, 4 and 5. The *JiNao Report* disclosed the monitoring of different types of OSPF packets, several of which correspond to the claimed measure categories. *See JiNao Report* at 19 [Ex. J]. For example, the monitored "Link State Request" packets are used to request up-to-date pieces of a neighbor's database, and thus constitute a "network packet data transfer command" as required by '338 claim 2.[104] The monitored "Hello" packets are sent periodically to establish and maintain neighbor relationships, or connections, and thus constitute both a measure of "network connections" and also a "network connection request" as required by '338 claim 5.[105]

In addition, the *JiNao Report* also directs the reader to monitor "network packet data transfer volume" as required by '338 claim 4. For example, the *JiNao Report* states:

> The activity intensity measures determine whether the **volume of general activity** generated in the recent past (depending on the half-life of the measure, here "recent past" corresponds to the time span of last several half-lifes) is normal.

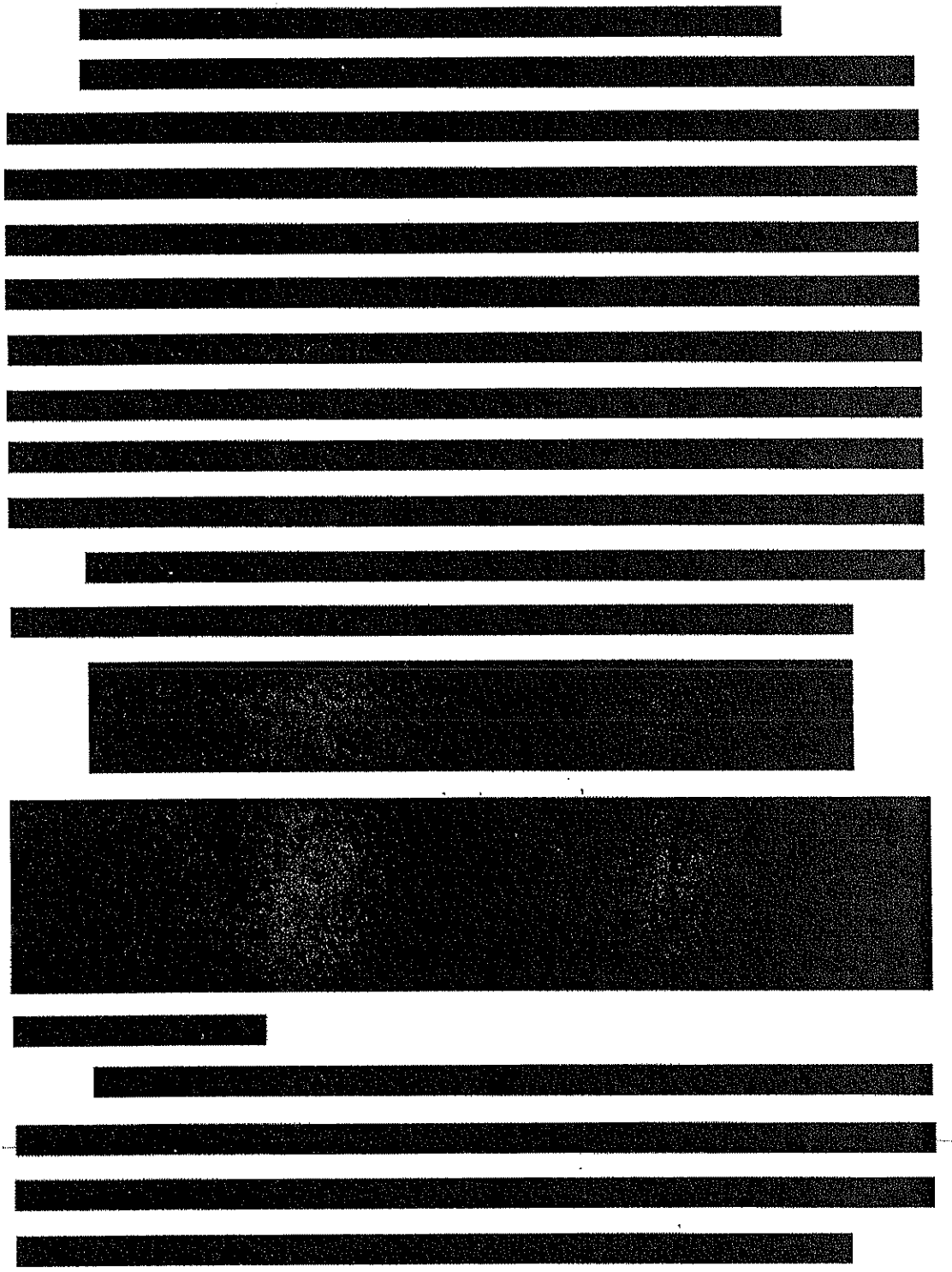
JiNao Report at 19 (emphasis added) [Ex. J]. One of the authors of the *JiNao Report*, Mr. Jou, agreed that this text disclosed using data volume as a measure.[106] Thus, as shown in Exhibit M, all of the asserted '338 claims are invalided by the *JiNao Report*.

---

[104] *See* RFC 2328 <http://www.ietf.org/rfc/rfc2328.txt?number=2328> at SYM_P_0604975 (describing Link State Request packet) and at SYM_P_0604583-604 (describing OSPF packets generally) [Ex. OO].

[105] *Id.* at SYM_P_0604967 (describing OSPF Hello packets) [Ex. OO].

[106] Jou Tr. 164-65 [Ex. R].



Dated: June 16, 2006

POTTER ANDERSON & CORROON LLP

/s/ Richard L. Horwitz
Richard L. Horwitz (#2246)
David E. Moore (#3983)
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19899
Tel.: (302) 984-6000
Fax: (302) 658-1192

OF COUNSEL:

Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
1180 Peachtree Street
Atlanta, GA 30309
Tel: (404) 572-4600
Fax: (404) 572-5134

Theresa A. Moehlman
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100
Fax: (212) 556-2222

Attorneys for Defendant
INTERNET SECURITY SYSTEMS, INC.,
a Delaware Corporation and
INTERNET SECURITY SYSTEMS, INC.,
a Georgia Corporation

MORRIS, JAMES, HITCHENS & WILLIAMS, LLP

Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
Tel.: (302) 888-6800

OF COUNSEL:

Lloyd R. Day, Jr.
Robert M. Galvin
Paul S. Grewal
DAY, CASEBEER MADRID & BATCHELDER LLP
20300 Stevens Creek Blvd.,
Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

Attorneys for Defendant
SYMANTEC CORPORATION

CERTIFICATE OF SERVICE

I hereby certify that on the 16th day of June, 2006, I electronically filed the foregoing document, **OPENING BRIEF IN SUPPORT OF JOINT MOTION FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 & 103 OF DEFENDANTS ISS AND SYMANTEC**, with/ the Clerk of the Court using CM/ECF which will send notification of such filing to the following:

John F. Horvath, Esq.
Fish & Richardson, P.C.
919 North Market Street, Suite 1100
Wilmington, DE 19801

Richard L. Horwitz, Esq.
David E. Moore, Esq.
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
Wilmington, DE 19801

Additionally, I hereby certify that on the 16th day of June, 2006, the foregoing document was served via email and via federal express on the following non-registered participants:

Howard G. Pollack, Esq.
Michael J. Curley, Esq.
Fish & Richardson
500 Arguello Street, Suite 500
Redwood City, CA 94063
650.839.5070

Holmes Hawkins, III, Esq.
King & Spalding
1180 Peachtree Street
Atlanta, GA 30309-3521
404.572.4600

Theresa Moehlman, Esq.
King & Spalding LLP
1185 Avenue of the Americas
New York, NY 10036-4003
212.556.2100

/s/ Mary M. Matterer
Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
Morris, James, Hitchens & Williams LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
(302) 888-6800
rherrmann@morrisjames.com
mmatterer@morrisjames.com
Counsel for Defendant Symantec Corporation

EXHIBIT 3

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants and Counterclaim-Plaintiffs.	Civil Action No. 04-CV-1199 (SLR) **FILED UNDER SEAL** THIS DOCUMENT CONTAINS MATERIALS WHICH ARE CLAIMED TO BE CONFIDENTIAL AND COVERED BY A PROTECTIVE ORDER. THIS DOCUMENT SHALL NOT BE MADE AVAILABLE TO ANY PERSON OTHER THAN THE COURT AND OUTSIDE COUNSEL OF RECORD FOR THE PARTIES)

DEFENDANTS' JOINT REPLY BRIEF IN SUPPORT OF THEIR MOTION FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 & 103

Richard K. Herrmann (#405)
Morris, James, Hitchens & Williams, LLP
222 Delaware Avenue, 10th Floor
P.O. Box 2306
Wilmington, DE 19899-2306
Tel: (302) 888-6800
Fax: (302) 571-1751

Attorneys for Defendant and Counterclaim Plaintiff Symantec Corporation

OF COUNSEL:

Lloyd R. Day, Jr. (*pro hac vice*)
Robert M. Galvin (*pro hac vice*)
Paul S. Grewal (*pro hac vice*)
Day Casebeer Madrid & Batchelder LLP
20300 Stevens Creek Blvd., Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop (*pro hac vice*)

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

Dated: July 10, 2006

Table of Contents

I. INTRODUCTION

Based upon SRI's Answering Brief, very few issues remain in dispute with regard to the prior art at issue: *Emerald 1997*, *Live Traffic*, and *JiNao Report*. For each reference, SRI has conceded disclosure of most or all of the limitations of the claims necessary to find anticipation, and on the remaining points, SRI has not raised a genuine issue of material fact because they have not come forward with evidence sufficient for a reasonable trier of fact to find in its favor, even giving SRI the benefit of all reasonable inferences.

The uncontested issues and SRI's few remaining challenges are summarized below. Defendants have shown there is no genuine issue of material fact that would preclude summary judgment on all asserted claims. At a minimum, partial summary judgment of the following should be granted, which will significantly narrow the issues for trial.

[redacted]

4. *JiNao Report* discloses all but one of the limitations of the '338 claims.

   - SRI contests only the limitations "receiving network packets" and "from at least one measure of the network packets" which SRI concedes are synonymous, *i.e.*, if one is disclosed, both are disclosed.

[redacted]

II. SUMMARY JUDGMENT OF INVALIDITY SHOULD BE ENTERED ON ALL OF THE ASSERTED CLAIMS

A. LEGAL STANDARDS

Summary judgment is appropriate here because SRI has failed to come forward with specific material facts showing a genuine issue for trial. "Facts that could alter the outcome are material, and disputes are genuine if evidence exists from which a rational person could conclude that the position of the person with the burden of proof on the disputed issue is correct." *Matsushita Elec. Indus. Co. v. Cinram Int'l, Inc.*, 299 F. Supp. 2d 348, 357 (D. Del. 2004) (citations omitted).

[redacted]

Pages 3 through 13

Redacted

[redacted]

D. THE JINAO REPORT ANTICIPATES THE ASSERTED CLAIMS

SRI purports to contest *JiNao Report*'s disclosure of only one of the limitations of the '338 claims, [redacted] As explained in detail below, the rest of SRI's arguments, while styled as challenging the "disclosure" of an additional limitation of the hierarchical patents, are actually enablement arguments.

[redacted]

1. The JiNao Report anticipates the asserted '338 claims

The only limitation of the '338 claims that SRI alleges is not disclosed by the *JiNao Report* is building statistical profiles "from at least one measure of the network packets."[44] As support for this proposition, SRI attempts to suggest that JiNao used audit records, rather than network packets, as its data source. But *JiNao Report* repeatedly discloses that "measures" are built from network packets. The JiNao authors characterized one type of these network packet measures as an "audit record distribution measure" because JiNao used the NIDES algorithms, and this was the name of one of the four measures used in NIDES.[45] This does not change the fact, however, that the *JiNao Report* clearly discloses analysis of network traffic and network packets, and the creation of statistical profiles based upon received packets.

SRI claims that the JiNao system was akin to the "early systems focused on the analysis of audit logs."[46] But the introduction of the *JiNao Report* specifically distinguishes JiNao from analysis of host audit trails and explains that JiNao ***looks at network traffic***:

> In the early stage, intrusion detection system [sic] were designed around the analysis of a single host's audit trail. With the proliferation of computer networks, many of the intrusion detection systems began to extend the techniques to networks of computers. Most of the current network intrusion detection efforts have taken one of the two following approaches. One approach is to collect data from separate hosts on a network for processing by a centralized intrusion detection system [2][3]. The other approach is to target network traffic at the service and protocol levels [6][7]. Our effort is close to the second approach with a few exceptions. First we are interested in protecting network infrastructure and particularly focus on routing and management capabilities. Therefore, the target of analysis is mainly on specific protocol traffic instead of general data traffic.[47]

The *JiNao Report* states that JiNao ***receives*** network packets and uses them to create measures:

[redacted]

[44] Res. Br. at 25 [D.I. 339]. SRI treats the additional limitation of "receiving network packets" as synonymous with this limitation. Res. Br. at 27 [D.I. 339].

[45] *See Statistical Methods* at 307 (stating "NIDES uses four classes of measures: activity intensity, audit record distribution, categorical, and continuous.") [D.I. 301, Ex. FF].

[46] Res. Br. at 26 [D.I. 339].

> Measures: Aspects of subject behavior are represented as measures (e.g., ***packet*** and LSA arrival frequencies in terms of their types or sources). For each measure, we will construct a probability distribution of short-term and long-term behaviors. For example, ***for the packet types received, the long-term probability distribution would consist of the historical probabilities with which different types of packets have been received***, and the short-term probability distribution would consist of the recent probabilities ***with which different types of packets have been received***.[48]

The *JiNao Report* discusses packets and the receipt of packets repeatedly.[49]

The *JiNao Report* explains that for purposes of applying the NIDES algorithms, these measures based upon received packets are ***classified*** into different categories taken from the NIDES algorithms:

> In this case, the categories to which probabilities are attached are the names of packet types, which are learned by the system as they are received. ***We would classify the Ji-Nao measures into two groups***: activity intensity and audit record distribution measures.[50]

Even the mathematical formulae for computing the "audit record distribution measures" makes it clear that this measure is built using received packets. *See JiNao Report* at 21 ("$W_{m,j}$ is the number of packets received on the j^{th} day...")[51] *See also* the Declaration of L. Todd Heberlein for further explanation of the use of the term "audit" in the intrusion detection field.[52]

SRI's expert's attempt to distinguish JiNao as merely "reacting" to network packets strains all credibility and fails to raise a ***genuine*** issue of material fact. Even Dr. Kesidis himself

---

[47] *JiNao Report* at 2 [D.I. 301, Ex. J].

[48] *JiNao Report* at 19 (emphasis added) [D.I. 301, Ex. J].

[49] *JiNao Report* at 3 ("A local subsystem is associated with a router/switch to function as a security filter and ***analyze the incoming packets*** from its neighbors."), at 5 ("***If a packet passes through the prevention module, it will be forwarded*** to the protocol engine for execution and to the local detection module which performs both statistical- and protocol-based intrusion checks), and at 8, 14, 15, 16, 18, 21, 22, 24, 25 [D.I. 301, Ex. J]. *See also* the JiNao System Architecture diagram reproduced *infra* at 54, which shows the JiNao Module receiving input directly from the network.

[50] *JiNao Report* at 19 (emphasis added) [D.I. 301, Ex. J].

[51] D.I. 301, Ex. J.

[52] *See* Declaration of L. Todd Heberlein at ¶¶ 4-13.

was unable to "keep the story straight," necessitating SRI's three-page attempt to explain away his testimony. And, even then, Dr. Kesidis came to the conclusion that JiNao received network packets: "[JiNao] reacted to packets that are -- certain packets that are received by the router. So in the sense that it reacts to those packets, it receives them."[53] SRI's failure to even address, much less rebut, the disclosures above means the issue is ripe for summary judgment in Defendants' favor.

[redacted]

[53] Res. Br. at 28 [D.I. 339]; Compton Decl. Ex. H at 50:16-51:4 [D.I. 340].

[redacted]

Pages 18 and 19

Redacted

[redacted]

III. CONCLUSION

Since the systems and methods claimed in the asserted claims of the [redacted] were described in printed publications more than one year before their date of application for patent, Defendants are entitled to summary judgment pursuant to 35 U.S.C. § 102 [redacted] that the claims are invalid as a matter of law.

[redacted]

Dated: July 10, 2006

POTTER ANDERSON & CORROON LLP

Richard L. Horwitz (#2246)
David E. Moore (#3983)
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19899
Tel.: (302) 984-6000
Fax: (302) 658-1192

OF COUNSEL:

Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
191 Peachtree Street
Atlanta, GA 30303
Tel: (404) 572-4600
Fax: (404) 572-5145

Theresa A. Moehlman
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100
Fax: (212) 556-2222

Attorneys for Defendant
INTERNET SECURITY SYSTEMS, INC.,
a Delaware Corporation and
INTERNET SECURITY SYSTEMS, INC.,
a Georgia Corporation

MORRIS, JAMES, HITCHENS & WILLIAMS, LLP

Richard K. Hermann (#405)
Mary B. Matterer (#2696)
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
Tel.: (302) 888-6800

OF COUNSEL:

Lloyd R. Day, Jr.
Robert M. Galvin
Paul S. Grewal
DAY, CASEBEER MADRID & BATCHELDER LLP
20300 Stevens Creek Blvd.,
Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

Attorneys for Defendant
SYMANTEC CORPORATION

CERTIFICATE OF SERVICE

I hereby certify that on the 10th day of July, 2006, I electronically filed the foregoing document, **DEFENDANTS' JOINT REPLY BRIEF IN SUPPORT OF THEIR MOTION FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 & 103,** with the Clerk of the Court using CM/ECF which will send notification of such filing to the following:

John F. Horvath, Esq.
Fish & Richardson, P.C.
919 North Market Street, Suite 1100
Wilmington, DE 19801

Richard L. Horwitz, Esq.
David E. Moore, Esq.
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
Wilmington, DE 19801

Additionally, I hereby certify that on the 10th day of July, 2006, the foregoing document was served via email on the following non-registered participants:

Howard G. Pollack, Esq.
Michael J. Curley, Esq.
Fish & Richardson
500 Arguello Street, Suite 500
Redwood City, CA 94063
650.839.5070

Holmes Hawkins, III, Esq.
King & Spalding
191 Peachtree St.
Atlanta, GA 30303
404.572.4600

Theresa Moehlman, Esq.
King & Spalding LLP
1185 Avenue of the Americas
New York, NY 10036-4003
212.556.2100

/s/ Richard K. Herrmann
RICHARD K. HERRMANN (#405)
MARY B. MATTERER (#2696)
Morris, James, Hitchens & Williams LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
(302) 888-6800
rherrmann@morrisjames.com
mmatterer@morrisjames.com
Counsel for Symantec Corporation

EXHIBIT 4

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants and Counterclaim- Plaintiffs.	**CONFIDENTIAL** **FILED UNDER SEAL** Civil Action No. 04-CV-1199 (SLR)

DECLARATION OF RENEE DUBORD BROWN IN SUPPORT OF DEFENDANT'S JOINT MOTION FOR SUMMARY JUDGMENT REGARDING INVALIDITY

I, Renee DuBord Brown, declare as follows:

1. I am a member of the law firm of Day Casebeer Madrid & Batchelder LLP, counsel for Defendant Symantec Corporation. I am admitted to practice law before all courts of the State of California.

2. I make this declaration of my own personal knowledge. If called to testify as to the truth of the matters stated herein, I could and would do so competently.

3. Attached hereto as Exhibit A is a true and correct copy of U.S. Patent No. 6,321,338.

[redacted]

[redacted]

12. Attached hereto as Exhibit J is a true and correct copy of Y. Frank Jou et al., *Architecture Design of a Scalable Intrusion Detection System for the Emerging Network Infrastructure*, Technical Report, April 1997 (hereinafter "*JiNao Report*").

[redacted]

15. Attached hereto as Exhibit M is a chart comparing the asserted claims of the patents-in-suit to the disclosure of *JiNao Report*.

[redacted]

20. Attached hereto as Exhibit R is a true and correct copy of selected pages of the 01/27/2006 Deposition of Y. Frank Jou (hereinafter "Jou Tr."), as well as Exhibit J17 (SRIE 0399295) from the 01/27/2006 Deposition of Y. Frank Jou.

21. Attached hereto as Exhibit S is a true and correct copy of selected pages of the 4/17/06 Affidavit of Paul Hickman, Office Manager at the Internet Archive (hereinafter "Internet Archive Decl.").

22. Attached hereto as Exhibit T is a true and correct copy of selected pages of the 03/09/2006 and 03/10/2006 Deposition of Phillip Porras (hereinafter "Porras Tr.") and the 03/30/2006 30(b)(6) Deposition of Phillip Porras (hereinafter "Porras 30(b)(6) Tr.") as well as Exhibits SRI-3 (SRI 105589-609), SRI-26 (SRIE 0460761) and SRI-27 (SRI 094295) from the 03/30/2006 30(b)(6) Deposition of Phillip Porras.

23. Attached hereto as Exhibit U is a true and correct copy of selected pages of the 03/22/2006 and 03/23/2006 Deposition of Alfonso Valdes (hereinafter "Valdes Tr.").

24. Attached hereto as Exhibit V is a true and correct copy of selected pages of the 05/25/2006, 05/26/2006 and 05/29/2006 Deposition of George Kesidis (hereinafter "Kesidis Tr.").

[redacted]

26. Attached hereto as Exhibit X is a true and correct copy of the Declaration of Frederick Avolio (hereinafter "Avolio Decl.").

27. Attached hereto as Exhibit Y is a true and correct copy of the Declaration of L. Todd Heberlein (hereinafter "Heberlein Decl.").

28. Attached hereto as Exhibit Z is a true and correct copy of pages 7, 11, 18-19 and 74 of R. Bace, INTRUSION DETECTION (Macmillan Technical Publishing 2000).

29. Attached hereto as Exhibit AA is a true and correct copy of pages 289-292 and

638-639 of S. Garfinkel and G. Spafford, PRACTICAL UNIX & INTERNET SECURITY (O'Reilly and Assoc. 2nd ed. 1996).

[redacted]

33. Attached hereto as Exhibit EE are true and correct copies of documents bearing BATES Production Nos.: SRI 011739-SRI 011743; SRI 012308-SRI 012404.

34. Attached hereto as Exhibit FF is a true and correct copy of A. Valdes and D. Anderson, *Statistical Methods for Computer Usage Anomaly Detection Using NIDES (Next-Generation Intrusion Detection Expert System)*, Proceeding of the Third International Workshop on Soft Computing, Jan. 27, 1995 (hereinafter "*Statistical Methods*").

[redacted]

[redacted]

39. Attached hereto as Exhibit KK is a true and correct copy of selected pages of the 04/10/2006 Deposition of Teresa Lunt (hereinafter "Lunt Tr.").

40. Attached hereto as Exhibit LL is a true and correct copy of selected definitions from Computer Dictionary, Microsoft Press 3rd ed. (1997).

[redacted]

42. Attached hereto as Exhibit NN is a true and correct copy of L.T. Heberlein et al., *A Network Security Monitor*, Proceedings of the 1990 IEEE Computer Security Symposium on Research in Security and Privacy, Oakland, CA, May 7-9, 1990.

43. Attached hereto as Exhibit OO is a true and correct copy of selected pages of the Internet Standards Request for Comments 2328 "OSPF Version 2," April 1998, <http://www.ietf.org/rfc/rfc2328.txt?number=2328> (last visited June 13, 2006).

[redacted]

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct to the best of my knowledge.

Dated: June 16, 2006

By: Renee DuBord Brown
Renee DuBord Brown

[redacted]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants and Counterclaim-Plaintiffs.	Civil Action No. 04-CV-1199 (SLR)

EXHIBITS TO

OPENING BRIEF IN SUPPORT OF JOINT MOTION FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 & 103 OF DEFENDANTS ISS AND SYMANTEC

June 16, 2006

POTTER ANDERSON & CORROON LLP

Richard L. Horwitz (#2246)
David E. Moore (#3983)
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19899
Tel.: (302) 984-6000
Fax: (302) 658-1192
rhorwitz@potteranderson.com
dmoore@potteranderson.com

MORRIS, JAMES, HITCHENS & WILLIAMS, LLP
Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
Tel.: (302) 888-6800
rherrmann@morrisjames.com
mmatterer@morrisjames.com

OF COUNSEL:

Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
1180 Peachtree Street
Atlanta, GA 30309
Tel: (404) 572-4600
Fax: (404) 572-51345

Theresa A. Moehlman
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100
Fax: (212) 556-2222

Attorneys for Defendant
INTERNET SECURITY SYSTEMS, INC.,
a Delaware Corporation and
INTERNET SECURITY SYSTEMS, INC.,
a Georgia Corporation

OF COUNSEL:

Lloyd R. Day, Jr.
Robert M. Galvin
Paul S. Grewal
DAY, CASEBEER MADRID &
BATCHELDER LLP
20300 Stevens Creek Blvd.,
Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

Attorneys for Defendant
SYMANTEC CORPORATION